Exhibit 1

ICC Comments

FCC No. RM 10865

04/12/2004

U.S. Department of Justice
Federal Bureau of Investigation

Digital Telephony and Communications Privacy Improvement Act of 1994

A legislative proposal to protect the American public from criminal activity and ensure privacy in telecommunications.

2/94

DIGITAL TELEPHONY

AND

COMMUNICATIONS PRIVACY IMPROVEMENT ACT OF 1994

TABLE OF CONTENTS

For more information, please contact The Office of Public and Congressional Affairs at FBI Headquarters, Washington, D.C. telephone (202) 324-2727.

INTRODUCTION

This report by the Federal Bureau of Investigation discusses a major new problem facing the criminal justice system nation-wide: Advances in telecommunications technology that will make it virtually impossible for law enforcement agencies to conduct court-authorized electronic surveillance.

For the benefit of members of Congress and other public officials, the report contains a summary of the key matters involved in the "digital telephony" issue and proposes legislation that would enable law enforcement to conduct court-approved surveillance of communications systems containing the complex new technology.

The draft legislation is titled: "Digital Telephony and Communications Privacy Improvement Act of 1994." It is included in the report along with a section-by-section analysis and other material.

For additional information, please call the FBI's Office of Public and Congressional Affairs, 202-324-2727.

#####

DIGITAL TELEPHONY ISSUE

SUMMARY

Advanced telecommunications technologies threaten to cripple the government's ability to protect the nation against the worst and most dreaded crimes.

The Problem: When in widespread use, the technologies will make it virtually impossible for federal law enforcement agencies to use court-approved electronic surveillance.

The Answer: Congress must enact legislation requiring that the new technologies contain capabilities allowing the government to continue using this invaluable tool to safeguard the United States.

More than 25 years ago, Congress passed a law allowing court-authorized surveillance, and it has become one of the most valuable law enforcement techniques against the very worst crimes.

For example: From 1982 to 1992, more than 22,000 convictions resulted from 8,300 court-approved surveillances.

Without that tool, law enforcement's ability to protect the public will be permanently eroded and the national security will be gravely endangered.

Court-approved surveillance is the most important and often the only way to prevent or solve life-and-death crimes.

How grave are those crimes?

They appear often enough in newspapers and television broadcasts: Terrorism, espionage, other foreign threats, violent crime, organized crime, drug trafficking, kidnapping--and more.

In addition to the federal government, state and local law enforcement agencies also will be unable to carry out court-approved surveillance because of the new technologies.

That is why the nation's most important law enforcement organizations at the state and local level also firmly support protective legislation by Congress. They include the

International Association of Chiefs of Police, the National Sheriffs Association, the National Association of Attorneys General, and the National District Attorneys Association.

Law enforcement at the grass roots throughout the nation **and** federal law enforcement stand together on this issue. Their goal is to better protect the people of the United States from harm.

But even now, "digital telephony" is developing so rapidly that several hundred court-authorized surveillances already have been prevented by new technological impediments associated with advanced communications equipment.

New legislation would not endanger privacy rights. The government would be given the same surveillance authority it has had since Congress created the surveillance law in 1968.

Telephone companies and others would only be required to assist law enforcement as they have for the past quarter-century--only now it would be assistance concerning new, different technology.

Without legislation, the government will eventually become virtually helpless to defend the nation from both foreign and domestic threats.

The threats include terrorists with bombs, spies who steal our most sensitive secrets, traffickers importing vast amounts of drugs, kidnappers who prey on children, murder plots, and other grave violent crimes.

Congress must pass legislation that would ~~by~~ reasonable steps allow law enforcement to carry out court-approved surveillance despite the intricate new communications technology and equipment.

Otherwise, the nation will find itself facing even worse crime and national security problems--not only in the rest of this century but well into the next. Failure to act now will cause lasting problems for the safety and security of the American people.

#####

DIGITAL TELEPHONY

QUESTIONS & ANSWERS

1. Why do we need legislation now? Is there really a problem?

For nearly a decade, law enforcement has been encountering technological impediments to court-ordered electronic surveillance. As a result, a number of court orders have been frustrated in whole or in part. These impediments result from the deployment of advanced telecommunications systems which were designed without consideration for law enforcement's interception needs. These impediments prevent or hinder telephone companies from providing law enforcement with the access required to obtain the content of communications that are the subject of court orders. Over the last four years, the government has sought to obtain, without success, a firm commitment from the telecommunications industry to remove the impediments at a fixed, reasonable date in the future. Consequently, legislation is necessary to resolve this impasse. Further delays in correcting these technological impediments will unnecessarily jeopardize the personal safety and economic well-being of the American public. The longer the delay, the more expensive it will be to correct this serious problem and the longer society will be put at risk and effective law enforcement hampered.

2. Won't the removal of these impediments make the networks less secure and vulnerable to hackers, etc?

No. As with other specialized services and features included within the telecommunications networks, proper planning and design will ensure the integrity and security of the networks. Telephone companies already employ techniques which maintain system security and guard against network vulnerability. Removal of the impediments to court-authorized electronic surveillance can be accomplished in a manner consistent with strong systems security. In fact, the legislation contains a network security provision. We are confident that the telephone companies will continue their substantial efforts to prevent "hackers" and others from penetrating the telecommunications networks. Further, since such penetration efforts are considered serious crimes by the Federal government, they will continue to be prosecuted to the fullest extent of the law.

3. Won't this legislation increase wiretapping?

No. Existing Federal law prescribes a rigorous procedure which law enforcement must follow in order to obtain judicial authorization to conduct electronic surveillance. The proposed legislation does not change the legal requirements or the administrative procedures for obtaining a court order for electronic surveillance, nor does it alter the criminal penalties for unlawfully intercepting communications. The essential pur-

pose of the legislation is to clarify the nature and extent of the existing statutory obligation of telephone companies to provide law enforcement with "the technical assistance necessary to accomplish the interception."

4. Who will pay for removing the impediments?

The Federal government. The government recognizes that there will be costs involved with preserving the public safety, society's economic well-being, effective law enforcement, and the national security through law enforcement's ability to conduct court-ordered electronic surveillance. The proposed legislation makes it clear that the Federal government will compensate telephone companies for fair and reasonable costs incurred by them during the compliance period established in the legislation.

5. Does law enforcement really need to do wiretaps? Can't it get the same information from other sources?

Court-ordered electronic surveillance is a critically important and unique law enforcement investigative technique. In fact, the law only permits the use of court-ordered electronic surveillance when other investigative techniques will not suffice or are too dangerous. Although other investigative techniques are important, the use of electronic surveillance provides law enforcement with information and evidence that, as a rule, are unobtainable through other investigative techniques.

6. How many wiretaps does law enforcement conduct in a year?

Under the statutes that permit electronic surveillance in criminal matters, the combined number of electronic surveillance court orders executed in recent years by all Federal, state, and local law enforcement agencies has averaged around 800-900 per year. The effectiveness of this technique is noteworthy. Between 1982-1992, over 22,000 dangerous felons have been convicted as a direct result of executing some 8,300 court orders for electronic surveillance. Importantly, hundreds of lives have been saved, and thousands of criminal acts prevented, through the use of this critically important technique. Additionally, the economic benefit derived by law enforcement and society as a whole from the use of electronic surveillance (i.e., fines, recoveries, restitution, and economic loss prevented) is in the billions of dollars.

7. Won't this legislation affect our telecommunication industry's competitiveness?

No. By its very nature the legislation will ensure fairness, equal treatment, and a "level playing field" within the telecommunications industry by requiring all telephone companies operating in the U.S. to remove the impediments to electronic surveillance within three years. Further, similar governmental initiatives are now under way in a number of foreign countries

that are designed to maintain the electronic surveillance capabilities of law enforcement in those countries in use against drug cartels, organized crime, and terrorist groups. Thus, as the U.S. telecommunications industry, including equipment manufacturers and support service providers, meet their domestic responsibilities under this legislation, they will be in an excellent position to respond to new market opportunities abroad in meeting foreign law enforcement's electronic surveillance needs.

103rd Congress
2nd Session

DRAFT

2/17/94

S._____
[H.R._____]

IN THE SENATE
IN THE HOUSE OF REPRESENTATIVES

M._____ introduced the following bill; which was referred to the Committee on _____

A BILL

To ensure continued law enforcement electronic surveillance access to the content of wire and electronic communications and call setup information when authorized by law, to improve communications privacy protection, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. SHORT TITLE.

This Act may be cited as the "Digital Telephony and Communications Privacy Improvement Act of 1994."

SEC. 2. PURPOSE. The purpose of this Act is to clarify and define the responsibilities of common carriers, providers of common carrier support services, and telecommunications equipment manufacturers to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information under chapters 119 and 206 of title 18 and chapter 36 of title 50. Otherwise, except for the provisions in section 4, nothing in this Act is intended to alter any provision contained in the Federal electronic surveillance, pen register, or trap and trace statutes, or

those of any state or other jurisdiction. In particular, nothing herein is intended to enlarge or reduce the government's authority to lawfully intercept the content of communications or ins tall or use pen register or trap and trace devices, or to increase or decrease any criminal penalties for unlawfully intercepting the content of communications or installing or using pen register or trap and trace devices, or to alter the provisions regarding service provider assistance, payment for assistance, causes of action, civil liability, or good faith defenses.

The Act is further intended to improve communications privacy protection for cordless telephones, certain radio-based data communications and networks, communications transmitted using certain privacy-enhancing modulation techniques, and to clarify the lawfulness of quality control and service provision monitoring of electronic communications.

SEC. 3. COMMON CARRIER ASSISTANCE.

(a) New section. Chapter 109 of title 18, United States Code, is amended by adding the following new section:

"Sec. 2237. Common carrier assistance to government agencies.

"(a) Assistance requirements. Common carriers shall be required to provide forthwith, pursuant to court order or lawful authorization, the following capabilities and capacities in order to permit the government to conduct electronic surveillance and pen register and trap and trace investigations effectively:

"(1) The ability to execute expeditiously and simultaneously within a common carrier's system all court orders and lawful authorizations for the interception of wire and electronic communications and the acquisition of call setup information related to the facilities or services of subscribers of such common carrier;

"(2) the ability to intercept the content of communications and acquire call setup information concurrent with the transmission of the communication to or from the subscriber's facility or service that is the subject of the court order or lawful authorization, to the exclusion of any wire or electronic communication or call setup information of any other subscriber, notwithstanding the mobile nature of the facility or service that is the subject of the court order or lawful authorization or the use by the subscriber who is the subject of the court order or lawful authorization of any features offered by the common carrier;

"(3) the ability to intercept the content of communications and acquire call setup information unobtrusively and with a minimum of interference with any subscriber's telecommunications service; and

"(4) the ability to receive, in a generally available format, the intercepted content of communications and acquired call setup information at a location identified by the government distant from the facility that is the subject of the interception, from the interception access point, and from the

premises of the common carrier (except where emergency or exigent circumstances such as those described in 18 U.S.C. 2518(7), 2518 (11)(b), or 3125, or in 50 U.S.C. 1805(e), necessitate monitoring at the common carrier's premises).

"(b) Systems security. The government shall notify a common carrier of any interception of wire or electronic communications or any acquisition of call setup information that is to be effected within the premises of such common carrier pursuant to court order or lawful authorization. After notification, such common carrier shall designate an individual or individuals to activate such interception or acquisition forthwith. Such individual(s) shall be available at all times to activate such interceptions or acquisitions. Such interceptions or acquisitions effected within the premises of a common carrier may be activated only by the affirmative intervention of such individual(s) designated by such common carrier.

"(c) Compliance date. To the extent that common carriers providing service within the United States currently cannot fulfil the requirements set forth in subsection (a) of this section, they shall fulfil such requirements within three years from the date of enactment of this Act.

"(d) Cooperation of support service providers and equipment manufacturers. Common carriers shall consult, as necessary, in a timely fashion with appropriate providers of common carrier support services and telecommunications equipment manufacturers for the purpose of identifying any services or equipment, includ-

ing hardware and software, that may require modification so as to permit compliance with the provisions of this Act. A provider of common carrier support services or a telecommunications equipment manufacturer shall make available to a common carrier on a timely and priority basis, at a reasonable and cost-effective charge, any support service or equipment, including hardware and software, which may be required so as to permit compliance with the provisions of this Act.

"**(e) Enforcement.** The Attorney General shall have authority to enforce the provisions of subsections (a), (b), (c), and (d) of this section. The Attorney General may apply to the appropriate United States District Court for an order restraining or enjoining the provision of service of any common carrier who violates subsection (a), (b), (c), or (d) of this section and for an order mandating the cooperation of a provider of common carrier support services or a telecommunications equipment manufacturer pursuant to the provisions in subsection (d). The District Courts shall have jurisdiction to issue such orders. The Attorney General may also request the Federal Communications Commission to assist in enforcing provisions of this Act.

"**(f) Penalties.** Any common carrier that violates any provision of subsection (a) of this section shall be subject to a civil penalty of $10,000 per day for each day in violation. The Attorney General may file a civil action in the appropriate United States District Court to collect, and the United States District Courts shall have jurisdiction to impose, such

penalties. After consultation with the Attorney General, the Federal Communications Commission may also impose regulatory sanctions or fines otherwise authorized by law.

"(g) Consultation. The Attorney General is encouraged to consult with the Federal Communications Commission and common carrier representatives and to utilize common carrier standards bodies, associations, or other such organizations to discuss details of the requirements, such as those related to capacity, and cost-effective approaches in order to facilitate compliance with the provisions of this Act.

"(h) Funding. The Federal Government shall pay common carriers for reasonable and cost-effective charges directly associated with the modifications required to assure common carrier compliance with the requirements of this Act which are incurred within the three year period set for compliance.

"(i) Definitions. -- As used in this Section --

(1) 'common carrier' means any person or entity engaged as a common carrier for hire, as defined by section 3(h) of the Communications Act of 1934, and includes a commercial mobile service or interconnected service, as defined in section 6002(b) of Public Law 103-66;

(2) 'provider of common carrier support services' means any person or entity who provides services to a common carrier that are integral to processing, directing, forwarding, or completing telephone calls or electronic communication transmissions;

(3) 'wire communication' shall have the same meaning as set forth in subsection 2510(1) of title 18, United States Code;

(4) 'electronic communication' shall have the same meaning as set forth in subsection 2510(12) of title 18, United States Code;

(5) 'intercept' shall have the same meaning as set forth in section 2510(4) of title 18, United States Code, except that with regard to a common carrier's transmission of a communication encrypted by a subscriber, the common carrier shall not be responsible for ensuring the government agency's ability to acquire the plaintext of the communications content, unless the encryption was provided by the common carrier and the common carrier possesses the information necessary to decrypt the communication;

(6) 'concurrent with the transmission of the communication,' as used in section 3(a)(2) of this Act, means contemporaneous with the transmission; but it shall include, with regard to electronic communications, the ability of a government agency to acquire such communications at the conclusion of the transmission, and, with regard to call setup information, the ability to acquire such information either before, during, or immediately after the transmission of the communication;

(7) 'call setup information' shall mean the information generated which identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful

authorization, including information associated with any telecommunication system dialing or calling features or services; and

(8) 'government' means the Government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory or possession of the United States, and any state or political subdivision thereof authorized by law to conduct electronic surveillance."

SEC. 4. COMMUNICATIONS PRIVACY IMPROVEMENT AND MONITORING CLARIFICATION.

Chapter 119 of title 18 is amended by making the following changes:

(1) Cordless telephones.

(a) Definitions. - Section 2510 of title 18, United States Code, is amended

(1) in paragraph (1), by striking ", but such term does not include" and all that follows through "base unit"; and

(2) in paragraph (12), by striking subparagraph (A) and redesignating subparagraphs (B) through (D) as subparagraphs (A) through (C), respectively.

(b) Penalty. - Section 2511 of title 18, United States Code, is amended -

(1) in subsection (4)(b)(i), by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,"; and

(2) in subsection (4)(b)(ii), by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,".

(2) Radio based data communications.

Section 2510(16) of title 18, United States Code, is amended by striking the word "or" at the end of subparagraph (D) and inserting an "or" at the end of subparagraph (E) and adding the following new subparagraph:

"(F) an electronic communication;".

(3) Penalties for monitoring radio communications that are not scrambled, encrypted, or non-public.

Section 2511(4)(b) of title 18, United States Code, is amended by deleting the phrase "or encrypted, then--" and inserting the following:

", encrypted, or transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication, then--".

(4) Technical correction.

Section 2511(2)(a)(i) of title 18, United States Code, is amended by striking out "used in the transmission of wire communication" and inserting in lieu thereof "used in the transmission of a wire or electronic communication".